UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/764,682	01/23/2004	Brant L. Candelore	80398P252X3	9474

8791 7590 11/14/2008

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
BAYOU, YONAS A	

ART UNIT	PAPER NUMBER
2434	

MAIL DATE	DELIVERY MODE
11/14/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/764,682	CANDELORE, BRANT L.	
	Examiner	Art Unit	
	YONAS BAYOU	2434	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 August 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5-10,12,13,15-21 and 24-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5-10,12,13,15-21 and 24-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01/23/2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *04/23/2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to applicant's response filed on 08/18/2008.

2. Claims 1-3, 5-10, 12-13, 15-21 and 24-27 are pending.

3. Claims 4, 11, 14, 22-23 and 28-38 are cancelled.

4. Applicant's arguments have been fully considered but they are not persuasive.

5. When responding to the Office action, Applicant is advised to clearly point out the patentable novelty the claims present in view of the state of the art disclosed by the reference(s) cited or the objection made. A showing of how the amendments avoid such references or objections must also be present. See 37 C.F.R. 1.111(c).

Response to Arguments

1. Applicant, on pages 8 (para. 5) and 9 (paras.4-5), of the remarks, argues "Wasilewski does not teach mating key generator being a message that comprises an identifier of the supplier."

Examiner respectfully disagrees and asserts that Wasilewski discloses in FIG. 11 shows a CA message 805 which contains an EMM 1112. CA message 805 has a header 1003, a CA EMM message 1101, and a sealed digest 1103. CA EMM message 1101 consists of CA EMM message header 1105, EMM message 1107, and CRC error detection code 1109. EMM message 1107 in its turn contains EMM header 1113 and EMM.sub.-- inside.sub.-- data 1115. EMM.sub.-- inside.sub.-- data 115 is encrypted

using the public key of the DHCT 333 for which it is intended. The data which is encrypted is EMM data 1129, which in turn is made up of EMM.sub.-- inside.sub.-- header 1123 and EMM command.sub.-- data 1125 together with padding 1127. EMM data 1129 is also input to the MD5 one-way hash function to produce EMM MAC 1119 and sealed digest 1103 is made by encrypting EMM.sub.-- signing.sub.-- header 1117, EMM MAC 1119, EMM.sub.-- signing header 1117, and padding 1121 with the private key of either an entitlement agent or a conditional access authority, depending on what kind of EMM it is **[20:18-34 and fig. 11]**. The EMM.sub.-- signing.sub.-- header is information from the EMM.sub.-- inside.sub.-- header. This information is particularly sensitive and is consequently encrypted by both the public key of DHCT 333, for privacy reasons, and the private key of the entitlement agent or the conditional access authority, to apply a digital signature. Upon reception, and after the privacy decryption, if the signature verification fails, the EMM is discarded by DHCT 333. Included in this information are an ID for the conditional access system, the type of the CA message, the serial number of the microprocessor in the DHCT's DHCTSE 627, an identifier for the CAA or EA which is the source of the EMM, an indication of which of the three public keys for the CAA in DHCT 333's secure element is to be used to decrypt the sealed digest, and an indication of the format of the EMM. The contents of EMM command.sub.-- data 1125 will be explained in more detail in the discussion of the operations performed using EMMs **[20:35-52 and fig. 11;** see item: EMM 1112 = 1113 + 1115 + 1103].

2. Examiner, however, in light of the above submission maintains the previous rejections while considering the amendments to the claims as follows:

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-3, 5-10, 12-13, 15-21 and 24-27 are rejected under 35 U.S.C. 102(e) as being anticipated by Wasilewski US Patent No. 6,157,719 (hereinafter Wasilewski) .

Referring to claims 1, 3, 12 and 13, Wasilewski teaches a mating key gateway adapted to retrieve at least one mating key used to encrypt a program key that is used to scramble digital content prior to transmission to a digital device, comprising:

a bus **[column 14, lines 14-16** a bus is inherently a communication scheme (wires, fiber optics, fiber coax)];

a processor coupled to the bus **[column 21, lines 15-19 and fig. 12];**

an interface coupled to the bus, the interface being adapted to receive

information from (1) a sender of the digital content **[abstract**; programs are broadcast corresponding to send digital content] and (2) either a server controlled by a supplier of the digital device or a trusted third party, the information received by the interface from the sender comprises a mating key generator being a message that comprises an identifier of the supplier **[20:18-52 and fig. 11]**;and

a non-volatile storage unit coupled to the bus, the non-volatile storage unit to store a mating key lookup table to identify either the server controlled by the supplier of the digital device or the trusted third party based on the information received from the sender, from which the at least one mating key is supplied, the mating key lookup table stored by the non-volatile storage unit comprises (i) a first group of entries forming a range of mating key generators for digital devices supplied by each supplier of a plurality of suppliers including the supplier **[20:18-52 and fig. 11;** EMM inherently has a 64 bits mating key generator] , and (ii) a second group of entries corresponding to the first group of entries, each entry of the second group of entries including at least one mating key uniquely corresponding to and formed by at least a portion of one of the mating key generators **[25:3-26]**.

Referring to claim 2, Wasilewski teaches the mating key gateway, wherein the interface to receive the information from the sender being one of a cable provider, a satellite-based provider, a terrestrial-based provider, an Internet service provider and a conditional access (CA) provider operating with one of the cable provider, the satellite-

based provider, the terrestrial-based provider and the Internet service provider **[col. 15, lines 7-20 and fig. 6]**.

Referring to claims 5 and 25, Wasilewski teaches the mating key gateway inherently the security content delivery system, wherein the mating key generator received by the interface further comprises an identifier of a provider of a system that enables transmission of both the digital content and the mating key generator to the digital device **[col. 15, lines 7-20; col. 20, lines 35-50** (CAA corresponding to supplier/service provider)**; col. 24, lines 21-34; col. 35, lines 44-54; col. 41, lines 23-34; col. 46, lines 33-43 and fig. 6**].

Referring to claims 6, 15 and 26, Wasilewski teaches the mating key gateway, wherein the mating key generator received by the interface further comprises (i) an identifier that identifies a conditional access (CA) system provider over which the digital content and the mating key generator are transmitted **[col. 7, lines 7-11; col. 20, lines 35-50; col. 22, lines 23-42; col. 24, lines 21-34; col. 41, lines 47-67]**, and (ii) a mating key sequence number **[col. 24, lines 21-34; fig.6]**.

Referring to claims 7, 16 and 17, Wasilewski teaches the mating key gateway, wherein the mating key lookup table stored by the non-volatile storage unit comprises (i) a first group of entries forming a range of serial numbers for digital devices supplied by each supplier of a plurality of suppliers including the supplier **[20:18-52 and fig. 11]**,

and (ii) a second group of entries corresponding to the first group of entries, each entry of the second group of entries including information to establish communications with a server controlled by one of the plurality of suppliers **[25:3-26]**.

Referring to claims 8, 10 and 19, Wasilewski teaches the mating key gateway, wherein the mating key lookup table stored by the non-volatile storage unit comprises (i) a first group of entries forming a range of serial numbers for digital devices supplied by each supplier of a plurality of suppliers including the supplier **[20:18-52 and fig. 11]**., and (ii) a second group of entries corresponding to the first group of entries, each entry of the second group of entries including an address to establish communications with a trusted third party authorized by one of the plurality of suppliers **[col. 4, line 64 - col. 5, line 13; col. 7, lines 7-11; col. 19, lines 39-54; col. 24, lines 21-60]**.

Referring to claims 9 and 18, Wasilewski teaches the mating key gateway,

wherein the mating key lookup table stored by the non-volatile storage unit comprises (i) a first group of entries forming a range of mating key generators for digital devices supplied by each supplier of a plurality of suppliers including the supplier and the at least one mating key being formed using at least a portion of one of the mating key generators **[20:18-52 and fig. 11]**, and (ii) a second group of entries corresponding to the first group of entries, each entry of the second group of entries including information to establish communications with a server controlled by one of the plurality of suppliers **[25:3-26]**.

Referring to claim 20, Wasilewski teaches the mating key gateway being adapted to additionally store mating keys for selected digital devices **[col. 7, lines 7-11; col. 15, lines 59-67]**.

Referring to claim 21, Wasilewski teaches a secure content delivery system comprising:

a trusted third party to store a plurality of mating keys associated with digital devices, each mating key being used to encrypt a key that is used to scramble digital content **[col. 7, lines 7-11; col. 15, lines 59-67; col.22, lines 23-35; fig. 6**; a control suite 607 (equivalent to a trusted third party) stores keys/mating keys which inherently used to encrypt digital content];

a mating key gateway in communications with the trusted third party, the mating key gateway to provide information received from a head end to the trusted third party for retrieval of a requested mating key that is computed using the information received from the head end **[col. 7, lines 27-56; col.15, lines 7-23; col. 16, lines 47-55 and figs. 5-6]**.

Referring to claim 24, Wasilewski teaches a secure content delivery system, wherein the identifier of a supplier included in the mating key generator identifies a manufacturers of the one of the digital devices **[20:18-52 and fig. 11]**.

Referring to claim 27, Wasilewski teaches a method comprising:

receiving a mating key **[col. 7, lines 7-11]**;

receiving a serial number being used to locate the one-time programmable value **[col. 7, lines 7-11; col. 7, line 65 – col. 8, line 28]**;

computing a mating key by performing a computation on the mating key generator and the one-time programmable value to produce the mating key **[col. 25, lines 4-26]**; and

outputting the mating key based on the mating key generator being a message including at least one of (i) a first identifier to identify a manufacturer of the digital device, (ii) a service provider identifier, and (iv) a mating key sequence number and the one-time programmable value being identical to a key stored in a digital device of a set-top box targeted to receive information encrypted with either the mating key or a derivative of the mating key **[20:18-52 and fig. 11]**.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to YONAS BAYOU whose telephone number is (571)272-7610. The examiner can normally be reached on m-f,7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571-272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Yonas Bayou/

Examiner, Art Unit 2434

11/08/2008

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2434